

Play It Safe: Manage Security Risks Introduction to Cert 2

My name is Ashley, and I'm a Customer Engineering Enablement Lead for Security Operation Sales at Google. I'm excited to be your instructor for this course.

Let's start by quickly reviewing what we've covered so far. Earlier, we defined security and explored some common job responsibilities for entry-level analysts. We also discussed core skills and knowledge that analysts need to develop. Then, we shared some key events like the LoveLetter and Morris attacks that led to the development and ongoing evolution of the security field. We also introduced you to frameworks, controls, and the CIA triad, which are all used to reduce risk.

In this course, we'll discuss the focus of Certified Information Systems Security Professional's, or CISSP's, eight security domains. We'll also cover security frameworks and controls in more detail, with a focus on NIST's Risk Management Framework. Additionally, we'll explore security audits, including common elements of internal audits. Then, we'll introduce some basic security tools, and you'll have a chance to explore how to use security tools to protect assets and data from threats, risks, and vulnerabilities.

Securing an organization and its assets from threats, risks, and vulnerabilities is an important step in maintaining business operations. In my experience as a security analyst, I helped respond to a severe breach that cost the organization nearly \$250,000. So, I hope you're feeling motivated to continue your security journey. I know I'm excited. Let's get started!

Revision #1

Created 3 June 2023 04:55:48 by naruzkurai

Updated 3 June 2023 04:56:12 by naruzkurai